

In The Claims:

Please cancel without prejudice claims 12-13 and 28-29.

Please amend the remaining claims as follows:

- 1 1. (currently amended) A disk drive comprising:
- 2 (a) a disk for storing data including embedded servo sectors comprising servo bursts, the
- 3 disk comprising a public area for storing plaintext data and a pristine area for storing
- 4 encrypted data;
- 5 (b) a head for reading the encrypted data from the pristine area of the disk;
- 6 (c) a control system for interfacing with a host computer to facilitate read and write
- 7 commands to write data to and read data from the pristine area of the disk, the control
- 8 system comprising:
- 9 authentication circuitry for authenticating a request received from the host
- 10 computer to access the pristine area of the disk;
- 11 a secret drive key; ~~and~~
- 12 decryption circuitry, responsive to the secret drive key, for decrypting the
- 13 encrypted data stored in the pristine area of the disk to generate decrypted
- 14 data; and
- 15 a servo control system responsive to the embedded servo sectors;
- 16 wherein:
- 17 the servo bursts are written to the disk in encrypted form; and
- 18 the authentication circuitry enables the servo control system to decrypt the servo
- 19 bursts.

- 1 2. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted
- 2 authentication data.

- 1 3. (original) The disk drive of claim 2, wherein the authentication circuitry is responsive to
2 the decrypted data.
- 1 4. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted user authentication data.
- 1 5. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted device authentication data for authenticating a device, the device comprising a
3 unique device ID configured during manufacture of the device.
- 1 6. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted information for implementing a challenge and response verification sequence.
- 1 7. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted message authentication data.
- 1 8. (original) The disk drive of claim 7, wherein the encrypted authentication data comprises
2 encrypted key data for generating a message authentication code.
- 1 9. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted key
2 data for decrypting an encrypted message.
- 1 10. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted
2 message data.
- 1 11. (original) The disk drive of claim 1, wherein the disk drive further comprises encryption
2 circuitry for encrypting plaintext data into the encrypted data stored in the pristine area.

1 12. (canceled)

1 13. (canceled)

1 14. (currently amended) The disk drive of ~~claim 13~~claim 1, wherein:

2 (a) the servo bursts are written to the disk with additive noise generated from a pseudo
3 random sequence;

4 (b) the pseudo random sequence is generated from a polynomial;

5 (c) the servo control system uses the polynomial to decrypt the servo bursts; and

6 (d) the authentication circuitry provides the polynomial to the servo control system.

1 15. (canceled)

1 16. (canceled)

1 17. (currently amended) A method of processing a request received by a disk drive from a
2 host computer to access encrypted data stored in a pristine area of a disk, wherein the
3 disk further comprises embedded servo sectors comprising servo bursts, the method
4 comprising the steps of:

5 (a) using a control system internal to the disk drive to receive the request from the host
6 computer;

7 (b) using the control system internal to the disk drive to authenticate the request to access
8 the pristine area and to enable access to the pristine area if the request is
9 authenticated;

10 (c) using the control system internal to the disk drive to read the encrypted data stored in
11 the pristine area; and

(d) using the control system internal to the disk drive to decrypt the encrypted data using a secret drive key within the disk drive to generate decrypted data;

(e) using the control system internal to the disk drive to servo a head over the disk in response to the embedded servo sectors; and

(f) using the control system internal to the disk drive to enable servoing in the pristine area if the request is authenticated,

wherein:

the servo bursts are written to the disk in encrypted form; and

the step of authenticating the request to access the pristine area comprises the step of decrypting the servo bursts.

18. (original) The method as recited in claim 17, wherein the encrypted data comprises encrypted authentication data.

19. (original) The method as recited in claim 18, wherein the step of authenticating is responsive to the decrypted data.

20. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted user authentication data.

21. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device.

22. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted information for implementing a challenge and response verification sequence.

1 23. (original) The method as recited in claim 18, wherein the encrypted authentication data
2 comprises encrypted message authentication data.

1 24. (original) The method as recited in claim 23, wherein the encrypted authentication data
2 comprises encrypted key data for generating a message authentication code.

1 25. (original) The method as recited in claim 17, wherein the encrypted data comprises
2 encrypted key data for decrypting an encrypted message.

1 26. (original) The method as recited in claim 17, wherein the encrypted data comprises
2 encrypted message data.

1 27. (original) The method as recited in claim 17, further comprising the step of encrypting
2 plaintext data to generate the encrypted data stored in the pristine area.

1 28. (canceled)

1 29. (canceled)

1 30. (currently amended) The method as recited in ~~claim 29~~claim 17, wherein:

2 (a) the servo bursts are written to the disk with additive noise generated from a pseudo
3 random sequence;

4 (b) the pseudo random sequence is generated from a polynomial; and

5 (c) the step of servoing uses the polynomial to decrypt the servo bursts.

1 31. (currently amended) A method of processing a request received by a disk drive from a
2 host computer to access data stored on a disk, the disk comprising a public area for
3 storing plaintext data and a pristine area for storing encrypted data, the disk further
4 comprises embedded servo sectors comprising servo bursts, the method comprising the
5 steps of:
6 (a) using a control system internal to the disk drive to receive the request from the host
7 computer;
8 (b) using the control system internal to the disk drive to decrypt the encrypted data stored
9 in the pristine area of the disk using a secret drive key within the disk drive to
10 generate decrypted data; and
11 (c) using the control system internal to the disk drive to process the decrypted data to
12 authenticate the request received from the host computer before allowing access to
13 the disk;
14 (d) using the control system internal to the disk drive to servo a head over the disk in
15 response to the embedded servo sectors; and
16 (e) using the control system internal to the disk drive to enable servoing in the pristine
17 area if the request is authenticated.
18 wherein:
19 the servo bursts are written to the disk in encrypted form; and
20 the step of authenticating the request to access the pristine area comprises the step of
21 decrypting the servo bursts.

1 32. (currently amended) A disk drive comprising a disk for storing data including embedded
2 servo sectors comprising servo bursts, and a head for reading data from the disk, the
3 improvement comprising:

4 a control system for interfacing with a host computer to facilitate read and write
5 commands to write data to and read data from the disk, the control system
6 comprising:
7 authentication circuitry for authenticating a request received from the host computer
8 to access the disk;
9 a secret drive key; and
10 decryption circuitry, responsive to the secret drive key, for decrypting the encrypted
11 data stored on the disk to generate decrypted data; and
12 a servo control system responsive to the embedded servo sectors;
13 wherein:
14 the servo bursts are written to the disk in encrypted form; and
15 the authentication circuitry enables the servo control system to decrypt the servo
16 bursts.